Automating Entrust:

Improving Entrust Account Management at LANL

Leslie Geyer

Brenna Taylor

Los Alamos National Laboratory

June 11, 2007

Overview

- **Why do you care?**
- **What is Entrust?**
- **Why Entrust?**
- **LANL's dilemma**
- **Automating Entrust**

Encryption

- **Why is it needed?**
  - Security: Protecting data from those without a need-to-know, while at rest and potentially on the Inter/Intra-net
  - Identity Management: The management of a user's online credentials and access to systems. A means of electronically verifying users for data and system protection.

What is Entrust?

- **Entrust software allows encryption and digital signing of files and e-mail messages. Entrust is the encryption software DOE has chosen as the standard for data transmission and storage across the complex. It is available for both the open and classified networks at LANL.**

Why Use Entrust?

- **Established at LANL for many years**
- **PII crisis-- A well known issue that has now come to national attention**
- **Easiest, fastest implementation for protecting sensitive systems in the heterogeneous environment required at LANL**

LANL's Dilemma

- **The recent rise in the loss or compromise of unclassified systems containing personal data for government (and private sector) employees created the necessity to protect all LANL laptops containing Personal Identifying Information (PII)**

- **This would mean 500-5000 new Entrust accounts over a 2-3 month period, depending upon the final implementation**

- **The Entrust account management system in use prior to early Fall of 2006 had been setup for a small number of users and was in large part manual and time consuming for users, administrators, and trusted agents**

Automating Entrust

- **Overview of “old” entrust process**
- **Overview of “new” entrust process**
- **Examples of improved process**
- **Benefits of using existing account management database**
- **What was gained**
- **Areas for future improvement**

The “Old” Way

- **The players:**
  - Entrust Administrators
    - System administrators and programmers with access to the Entrust RA tool responsible for account management
  - Trusted Agents
    - Approved individuals located throughout the Laboratory who complete the necessary Visual Identification (VI) needed to distribute activation codes. Must be available/accessible to users to provide codes
  - Users
    - Protect documents, e-mails, and folders including PII using Entrust

The “Old” Way

- **A very time consuming process:**
  - Step 1
    - Users create an account via the online interface (est. 5 minutes)
  - Step 2
    - Users select a trusted agent from a list (*maintained manually*) and notify the Entrust Administrators via e-mail of selected agent, so activation codes can be sent to that agent and user (est. 2-4 hours, but this is generous)
  - !! Repeat Step 2, if selected agent is unavailable !!
  - Step 3
    - Entrust Administrator sends activation codes (in an Entrust encrypted e-mail) to the agent (est. 5 minutes)
    - Entrust Administrator sends reference number in clear text to potential user (est. 5 minutes)
  - Step 4
    - User and agent meet to complete the Visual ID, sign user’s agreement and distribute second half of activation codes (est. 1 hour - 1 month)

The “Old” Way, con’t

- **Caveats**
  - The whole process had to be repeated if it was not completed within a 2 week window
  - Trusted agents often required re-training for each user who selected them
  - Many areas of the Laboratory lacked trusted agents, which required the user to drive to some other location across campus

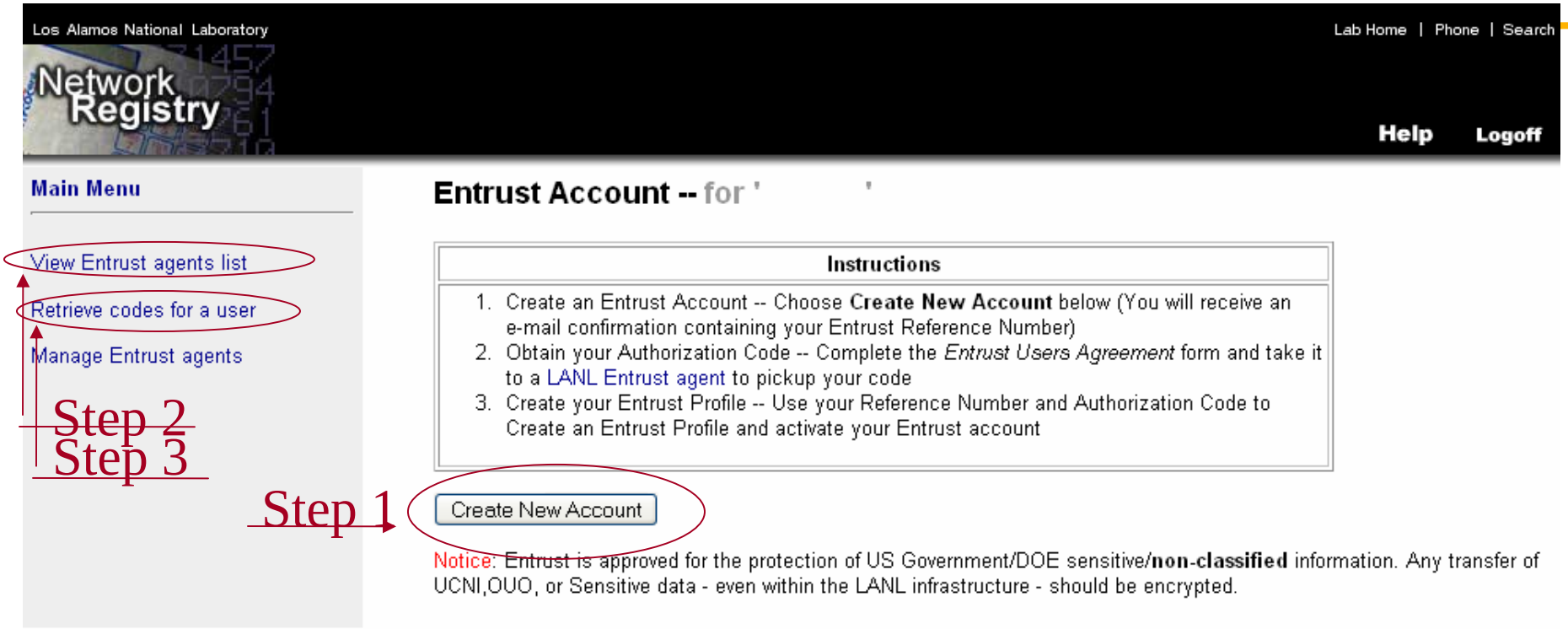
The “New” Way

- **The players:**
  - The same as before, only now much more of the process is self-service for users, and automatic for administrators and agents

The “New” Way

- **The new, improved process:**
  - Step 1
    - User creates an Entrust account through the online interface, one half of activation code is e-mailed to the user automatically (5 minutes)
  - Step 2
    - User contacts any of the listed agents (*list is generated dynamically with current data, many new agents added in the last year*) (5 minutes - 4 hours)
  - Step 3
    - Entrust agent completes Visual. ID and retrieves second half of activation codes from the online interface (*SSL encrypted*), user signs user agreement (5 minutes)

The “New” Way


Los Alamos National Laboratory
Network Registry
Lab Home | Phone | Search
Help Logoff
Main Menu
View Entrust agents list
Retrieve codes for a user
Manage Entrust agents
Step 2
Step 3
Step 1
Entrust Account -- for '
Instructions
1. Create an Entrust Account -- Choose Create New Account below (You will receive an e-mail confirmation containing your Entrust Reference Number)
2. Obtain your Authorization Code -- Complete the Entrust Users Agreement form and take it to a LANL Entrust agent to pickup your code
3. Create your Entrust Profile -- Use your Reference Number and Authorization Code to Create an Entrust Profile and activate your Entrust account
Create New Account
Notice: Entrust is approved for the protection of US Government/DOE sensitive/non-classified information. Any transfer of UCNI,OUO, or Sensitive data - even within the LANL infrastructure - should be encrypted.
Los Alamos National Laboratory • Est 1943
Operated by the Los Alamos National Security, LLC, for the
U.S. Department of Energy's National Nuclear Security Administration
Inside | © Copyright 2005–2006 LANSLLC All rights reserved | Disclaimer/Privacy |

The “New” Way

- **Other Improvements:**
  - Improved error messages and reporting to users and administrators
  - Automatic deactivation and archiving of terminated employees accounts
  - Automatic renewal of expired activation codes
    - *When requested through online interface*
  - More obvious options for updating Entrust password via the online interface
  - Trusted agent interface is a common interface used for other Identity Management tasks for all LANL users, thus more intuitive

Tying It Together

- **The “new” process:**
  - Interacts with LANL software licensing information to ensure that all Entrust users are licensed for their software

Tying It Together

- **The “new” process relies on an existing network account database to incorporate all necessary Entrust information with already established identity management.**
- **This allows:**
  - For real-time employee termination updates to automate the deactivation and archiving of Entrust accounts
  - Dynamic trusted agent listing with current location information

Overview of benefits

- **Time:**
  - Simpler user account creation and recovery
  - Thousands of process hours saved
- **Cost:**
  - Better use of server support resources -- no Admin involvement in sending out codes
  - Time savings allow all parties to work on other projects
  - Software license checks allow LANL to pay for only the Entrust licenses being used
- **Security:**
  - Better tracking of automated actions
  - Closer ties to institutional Identity Management system

Time savings breakdown

Hours and hours of human resource, end user and Administrator time:

- **New way of creating/re-issuing an account could take 15 minutes or less if trusted agent is local to the user**
- **Old way of creation/re-issuance required a minimum of 3-4 hours elapsed for a normal transaction (we'll use 4 hours for total elapsed time, but generally it took MUCH longer)**
- **1029 account creations from implementation (9/22/06) through April 30**
  - Before, 4116 hours of process time
  - Now, 257.25 hours of process time
  - Saved: 3,858.75 hours of process time
- **210 code reissues**
  - Before, 840 hours of process time
  - Now, 52.5 hours of process time
  - Saved: 787.5 hours of process time

Time savings breakdown (cont.)

892 recoveries: Old way allowed for automated recovery, so no time savings here; however, the improved interface is less confusing for the users

- **111 Deactivations:**
  - Before: 2 hours per 100 accounts
  - Now: 0 hours, no FTE manual time required now
  - Saved: 2 hours
- **88 errors (since tracking began):**
  - Before: Errors were untracked (estimate 30 minutes for error identification)t
  - Now: 15 minutes for error resolution
  - Saved: ~22 hours

Total Saved : 4,670.25 hours of process time

Areas for Improvement

- **Automating the reactivation of previously terminated Entrust accounts**
- **Expanding the number of Entrust agents in the field for users,**
- **Or, better yet, incorporating the visual ID into existing processes, and eliminating the requirement to do it again (i.e. when HR verifies your ID, a flag is set in the correct DB)**

Special Thanks

- **Other programmers and administrators from LANL Network Engineering that made this upgrade possible:**
  - Jeffrey Arbuckle
  - Cindy Eaton
  - Lynn Kluegel
  - Michael Lee
  - Jim Clifford
  - Silvia Hoisie

Questions